SonicOS

Hub and Spoke TZ170 VPNs with Checkpoint NG

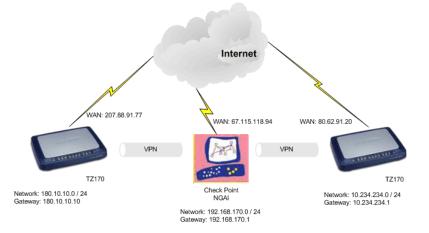
Introduction

This technote will detail all steps to get a Hub and Spoke setup between the SonicWALL SonicOS Enhanced and the Checkpoint NG. Within this setup the Checkpoint NG will be the HUB and 2 TZ170 units will be the Spokes.

Versions Used

- SonicOS 2.5.0.2 Enhanced on both TZ170 units
- Checkpoint FW-1 NGAI

Sample Diagram



Tasklist

On the SonicWALL units:

- Create new network objects and groups
- Create new VPN Policy for the Check Point FW-1 NG
- Specify Destination Network(s), IKE Phase 1 and Phase 2 properties

On FireWall-1 NG:

- Create local(Check Point) LAN network objects and group
- Create remote(SonicWALL's) LAN network objects
- Create new Interoperable Device objects
- Edit the Check Point Gateway object
- Verify the Topology
- Manually define VPN Domain
- Create new VPN Star Community
- Edit VPN Star community properties
- Verify Security Rules
- Verify Address Translation Rules

Testing

- Verify that traffic flows through the tunnel.
- Verify that applications function properly through the tunnel.
- Verify that the tunnel can reestablish if either side is disconnected.
- Verify that the network map and documentation match the running configuration.



Before You Begin

If you have not already done so, set up a management system connecting to the SonicWALL's internal LAN interface. The SonicWALL should already be configured for internet access; if not, do this before completing any further steps. The Check Point FireWall-1 NG server is also assumed to be properly configured for internet access.

Setup Steps

SonicWALL Setup Side Alice

Log into the SonicWALL's Management GUI using a current web browser.

SONICWALL		COMPRESENSIVE INTERNET SECURITY*
	Name:	admin
	Password:	Login x

The address objects will be created first, and then a group will be created to contain the address objects. From the navigation bar on the left, click on 'Network' and then 'Address Objects', this will bring up the 'Network > Address Objects' page. In the 'Address Objects' section, click on 'Add' to create the address objects for the networks connected to the Check Point FireWall-1 and SonicWALL. The first address object is for the LAN behind the Check Point FW-1.

System	SONICWALL		51c			
Network	System Petwork	Network > Address Objects				
🕿 Interfaces	riefers Wilffative LLB Zones	Address Croups vewther ("A areas clients (" clinic	m Address Unerth 🥤 Default Address Uberth			
💼 🗰 WAN Failover & LB	Address Doverb	- Baser	Address Datal	Tasar	Zano	Cosfigere
👼 Zones	Bill Routing	臣 田 LAN Sabrets		Graup		形象
📠 Zones	ALL AND PARCEN	TO BE WAAR Dollary to		Greup		20.8
📠 DNS	B DieCh Saver	T III CARE BUDINES		Orange		务组
Address Objects	P Helper	E = AUWON P		Group		96 B
Address Objects	- Anna Lawa	🗐 🗷 Allistetara P		Group		免息
📷 Routing		F E englek_genue		Greup		9.8
💼 NAT Policies		E ill machent_group		Griaup		外目
		Add Group				
💼 ARP		Address Objects				
💼 DHCP Server		- New	Address Datail	Type	2010	Cosfigure
🗰 IP Helper		E LAN Primary IP	192 188 168 168/255 251 255-255	Most	LAN	208
🕅 IP Helper		E Lourser Staret	192100-100-0/255266-256-6	Notwork	LAPE	2018
📖 Web Proxy		E YAN Prinay P	207.06.00.100236.255.256.255	PROST	TWNE	8.6
		T YMM Primary Satirut	237 88 91 64/255 251 255 224	Natives in	WWW	新商
Cine well		E 321F	102 100 100 3055 355 355 355	Hout	VMM	先年
Firewall		E Distant	192.168 180.0239 255 259 0	Detwork	YMAN	908
VPN		E RenadeAccess Newcra	04.06/06.9.0	Notveate	7718	95.8
V1 14		TT Vp+ D+D+D+C+++s	08060600	Raidwenn	VER	908
Users		E engest_ter	192 100 100 0/255 255 255 0	Network	LAN	99.8
	Freval	C checkpoint tax	102 168 170 0/265 264 255 0	Raphweeter Raphweeter	1982	9.8
Security Services	VITI	T angleture T panapoliture	192 160 189 00355 355 255 0 192 160 225 0255 355 255 0	Notweak	VP4	208 208
Log	Users	E senovel Jas	192 100 101 001 001 001 001 000	Norwen	LAN	20.0
LOG	Decirity Sections	All State	100 00 000 000 000 000		2.71	07-87
Help	i og Help	Act a were ablents (dam)				
Logout	Logovi Stater Ready	territori di constante di const				



Next create an address object group for the two checkpoint address objects. On the 'Network > Address Objects' page in the 'Address Groups' section, click on 'Add Group...' to create the address group for the objects.

🚰 Add Address Object	- Microsoft Internet Explorer 📃 🔲 🗙
Name:	checkpoint_lan
Zone Assignment:	VPN 🔽
Туре:	Network
Network:	192.168.170.0
Netmask:	255.255.255.0
Ready	
Keauy	
	OK Cancel

Name: checkpoint_lan Zone Assignment: VPN Type: Network Network: 192.168.170.0 Netmask: 255.255.255.0 Click 'OK' to finish.

🚰 Add Address Object	- Microsoft Internet Explorer 💶 🗙
Name:	Side_Bob_lan
Zone Assignment:	VPN 💌
Туре:	Network
Network:	10.234.234.0
Netmask:	255.255.255.0
Ready	
(nead)	
	OK Cancel

Name: Side_Bob_lan Zone Assignment: VPN Type: Network Network: 10.234.234.0 Netmask: 255.255.255.0 Click 'OK' to finish.

Next create an address object group for the two checkpoint address objects. On the 'Network > Address Objects' page in the 'Address Groups' section, click on 'Add Group...' to create the address group for the objects. The 'Name;" is "checkpoint_group"

🚰 Add Address Object Group - Microso	ft Internet Explorer	
Name: checkpoint_g	roup checkpoint_lan Side_Bob_Lan	
Ready		
	OK	

Select the "checkpoint_lan" object and 'Ctrl' or 'Shift' click to select the "Side_Bob_lan" object. Click the right arrow button to add both objects to the group.



From the navigation bar on the left, click on 'VPN', this will bring up the 'VPN > Settings' page. In the 'VPN Global Settings' section, make sure the 'Enable VPN' radio button is selected. In the 'VPN Policies' section, click on 'Add' to create the new VPN policy for the Check Point FireWall-1.

System	-				
Network	VPN > Settings		VPN Policy Wizard	Apply	Cancel ?
Wireless	VPN Global Settings				
Firewall	VPN Global settings				
VPN	Enable VPN				
) Settings	Unique Firewall Identifier: 0006B108	571D0			
Advanced					
DHCP over VPN	VPN Policies			Items 1	to 4 (of 4) [3] <] ▷ [
Local Certificates	📕 # Name	Gateway Destinati	ons Crypto Suite	Enable	Configure
CA Certificates	E 1 WAN GroupVPN	ducentry Destanda	ESP 3DES HMAC SHA1 (IKE)	Г	20 11 10
	2 LAN GroupVPN		ESP 3DES HMAC SHA1 (IKE)	Б	2000
	3 DMZ GroupVPN		ESP 3DES HMAC SHA1 (IKE)	П	200
	and contracto Variation				20 11 12
	4 WLAN GroupVPN		ESP 3DES HMAC SHA1 (IKE)	1	
Users	4 WLAN GroupVPN Add Celete		ESP 3DES HMAC SHA1 (IKE)	1.	Delete All
Security Services	Add Delete		ESP 3DES HMAC SHA1 (IKE)	1.:	-
Security Services Log		l, 14 Maximum Policies Allowed	ESP 3DES HMAC SHA1 (IKE)	1.	-
Security Services	Add Delete		ESP 3DES HIMAC SHA1 (IKE)		-

The 'VPN Policy' window will then appear. On the 'General' tab page, 'Security Policy' section, select "IKE using Preshared Secret" from the 'IPSec Keying Mode:' dropdown box.

VPN Policy - Mic	rosoft Internet E	kplorer				
General	Network	Proposals	Advanced			
Security P	olicy					
IPSec Keying	Mode:		IKE using Pre	shared Secret		
Name:			to_Checkpoint		_	
IPSec Primary	Gateway Name (or Address:	67.115.118.94		_	
IPSec Second	lary Gateway Nam	ne or Address:	0.0.0.0		_	
Shared Secre	t		HaRdI_to_Gue	66_Al1c3	_	
Local IKE ID (optional):	SonicWA	LL Identifier 💌	HUB-TEST		
Peer IKE ID (0	ptional):	IP Addres	is 💌	192.168.170.1		
Ready			_			
				OK	Cancel	Help

Name: "to_checkpoint"

IPSec Primary Gateway Name or Address: 67.115.118.94

Shared Secret: HaRd!_to_Gue55_Al1c3

Local IKE ID: SNWL Identifier HUB-TEST (the SonicWALL Identifier needs to be identical as the VPN SA name on the CheckPoint NG)

Peer IKE ID: IP Address 192.168.170.1



Next select the 'Network' tab.

VPN Policy - Microsoft Internet Explorer	
General Network Proposals Advanced	
Local Networks	
Choose local network from list LAN Primary Subnet	
O Local network obtains IP addresses using DHCP through this VPN Tunnel	
O Any address	
Destination Networks	
C Use this VPN Tunnel as default route for all Internet traffic	
C Destination network obtains IP addresses using DHCP through this VPN Tunnel	
Choose destination network from list checkpoint_group	
Ready	
OK Cancel Help	

In the 'Local Networks' section, select the radio button next to 'Choose local network from list' and select "LAN Primary Subnet" from the dropdown box.

In the 'Destination Networks' section, select the radio button next to 'Choose destination network from list' and select "checkpoint_group" from the dropdown box.

Next select the 'Proposals' tab. The default values should be correct, except the 'Life Time'; normally "28800" should be lowered to "3600" in both Phase 1 and 2 proposals. Verify that all values are correct.

Ø	/PN Policy - Microsoft Internet Explor	er			
	General Network P	oposals Advance	ed .		
	IKE (Phase 1) Proposal				
	Exchange:	Aggressive Mode	•		
	DH Group:	Group 5	•		
	Encryption:	3DES	•		
	Authentication:	SHA1	•		
	Life Time (seconds):	3600			
	Ipsec (Phase 2) Proposal				
		-			
	Protocol:	ESP	_		
	Encryption:	3DES	-		
	Authentication:	SHA1	•		
	Enable Perfect Forward Secrecy	,			
	DH Group:	Group 2	v		
	Life Time (seconds):	3600			
	Ready				
			ОК	Cancel	Help



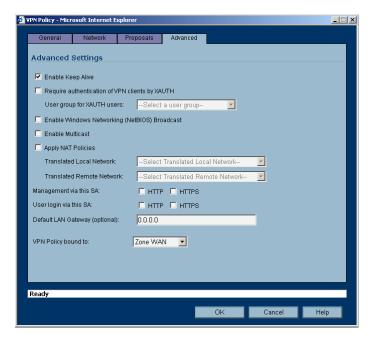
IKE (Phase 1) Proposal

Exchange: Aggressive Mode DH Group: Group 5 Encryption: 3DES Authentication: SHA1 Life Time (seconds): 3600

Ipsec (Phase 2) Proposal

Protocol: ESP Encryption: 3DES Authentication: SHA1 DH Group Group 2 Life Time (seconds): 3600 Do not enable Perfect Forward Security.

Next select the 'Advanced' tab.



Make sure that the option Enable Keep Alive is checked. All other options can be left as they are. Click the OK button.

This completes the settings on the SonicWALL TZ170 installed on Side Alice. Now, we will setup the Check Point unit we will setup the TZ170 unit at Side Bob.



SonicWALL Setup Side Bob

Log into the SonicWALL's Management GUI using a current web browser.



The address objects will be created first, and then a group will be created to contain the address objects. From the navigation bar on the left, click on 'Network' and then 'Address Objects', this will bring up the 'Network > Address Objects' page. In the 'Address Objects' section, click on 'Add' to create the address objects for the networks connected to the Check Point FireWall-1 and SonicWALL. The first address object is for the LAN behind the Check Point FW-1.

System	SONICWALL	Contraction property of the				
Network	System Returnic	Network > Address Objects				
🕿 Interfaces	Printerei WeitFatterei & LB Die Zones	Address Groups Vewton: CAI adress Obells C Cultur	n Addens Caseda 🥤 Default Addens Clavella			
💼 WAN Failover & LB	Address Dovets	- Disase	Address Detail	Type	Zano	Cosfigere
💼 Zones	Bi Houting	IT IS LAN Sabrets		Greup.	111	形象
	ALL AND PARCEN	TO DE WARE Extended		Greup		20.8
💼 DNS	B Dette Same	TT IS CRIZ SUBRETS		Orange		务组
📠 Address Objects 🛼	En Printpur	III III AIWAN P		Graup		96 B
	and the second	T 🗄 Allistation P		Oreup		免疫
💼 Routing 🏠		F Biergiek_genue		Greup		938
💼 NAT Policies		-E. B. mackpein_group		Grieug		9-18- 16-16-
		Addressy				
market ARP		Address Objects				
💼 DHCP Server			Address Detail	Type	Zenn	Cosfigare
📖 IP Helper		E LAN Primary IP	192 168 168 168(255 255 255 255	PROST	LAN	208
		E LANF Smary Subret	192 160 100 0/255 261 255 0	Notwork	Lini	20.00
💼 Web Proxy		IT YOU Prinary P	201 24 24 1 12230 255 259 255	PERST	TWNE	8.6
		IT matt Primary Saturet	207.00.01.64/255.255.255.224	Notwork	WWW	2018
Firewall		E 321P	102 100 200 3055 251 255 256	Heat	VMM	外市
Firewall		E District	192 168 19036250 255 259 0	Network	THEY	908
VPN		E ResumAccess Networks	06.06/06.0.0	Notyrein	NPIR	99.8
		IT VerDeDP Chierts	08060630	Radwards	VEH	908
Users		T engen_lan	192-166-600-0/255-255-255-0 192-160-170-0/255-264-255-0	Filefore de	VEN	死態 死後
	Preval	T anglet dree	102 100 100 00055 255 255 0	Namera	100g	20.8
Security Services	VITI	T Insingon Long	192 100 225 0/253 255 255 0	Network	VPH	20.0
Log	Users	T servered las	192 100 100 0058 255 255 0	Newsen	LAN	20.0
	THORY SECTOR	Alles				- AND THE REAL PROPERTY OF
Help	Log Help	Act a way address (dim.)				
Logout	Logov Stator: Ready					

Next create an address object group for the two checkpoint address objects. On the 'Network > Address Objects' page in the 'Address Groups' section, click on 'Add Group...' to create the address group for the objects.



🚰 Add Address Object	- Microsoft Internet Explorer 💶 🗙
Name:	checkpoint_lan
Zone Assignment:	VPN 🔽
Type:	Network
Network:	192.168.170.0
Netmask:	255.255.255.0
Ready	
Ready	
	OK Cancel

Name: checkpoint_lan Zone Assignment: VPN Type: Network Network: 192.168.170.0 Netmask: 255.255.255.0 Click 'OK' to finish.

Name:	Side_Alice_Lan
Zone Assignment:	VPN 💌
Туре:	Network
Network:	180.10.10.0
Netmask:	255.255.255.0
Ready	

Name: Side_Alice_lan Zone Assignment: VPN Type: Network Network: 180.10.10.0 Netmask: 255.255.255.0 Click 'OK' to finish.

Next create an address object group for the two checkpoint address objects. On the 'Network > Address Objects' page in the 'Address Groups' section, click on 'Add Group...' to create the address group for the objects. The 'Name;" is "checkpoint_group"

🚰 Edit Address Object Group - Microsoft Inter	het Explorer
Name: checkpoint_group	-> Checkpoint_lan Side_Alice_Lan
Ready	
	OK Cancel

Select the "checkpoint_lan" object and 'Ctrl' or 'Shift' click to select the "Side_Alice_lan" object. Click the right arrow button to add both objects to the group.

From the navigation bar on the left, click on 'VPN', this will bring up the 'VPN > Settings' page. In the 'VPN Global Settings' section, make sure the 'Enable VPN' radio button is selected. In the 'VPN Policies' section, click on 'Add' to create the new VPN policy for the Check Point FireWall-1.



System					
Network	VPN > Settings		VPN Policy Wizard	Apply	Cancel
Wireless Firewall	VPN Global Settings				
VPN	Enable VPN				
Settings	Unique Firewall Identifier: 0006B100	57100			
Advanced					
DHCP over VPN	VPN Policies			Items 1	to 4 (of 4) 🕄 🗸 🗅
	VPIN POlicies				
Local Certificates	# Name	Gateway Destinations	Crypto Suite	Enable	Configure
Local Certificates		Gateway Destinations	Crypto Suite ESP 3DES HMAC SHA1 (IKE)	Enable	Configure
Local Certificates	📕 # Name	Gateway Destinations		Service Service	and the second s
Local Certificates	 # Name 1 WAN GroupVPN 	Gateway Destinations	ESP 3DES HMAC SHA1 (IKE)	Б	888
Local Certificates	# Name 1 WAN GroupVPN 2 LAN GroupVPN	Gateway Destinations	ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE)	С С	\$19 \$ \$19 \$
Local Certificates	# Name 1 WAN Group/VPN 2 LAN Group/VPN 3 DMZ Group/VPN 4 WLAN Group/VPN	Gateway Destinations	ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE)		886 886 886
L2TP Server Local Certificates CA Certificates Users Users Security Services	# Name 1 WAN GroupVPN 2 LAN GroupVPN 3 DMZ GroupVPN 4 WLAN GroupVPN Add Crotete		ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE)		888 888 888
Local Certificates CA Certificates USers	# Name 1 WAN GroupVPN 2 LAN GroupVPN 3 DMZ GroupVPN 4 WLAN GroupVPN Add Crotete		ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE)		886 886 886
Local Certificates CA Certificates Users Security Services	# Name 1 WAN Group/VPN 2 LAN Group/VPN 3 DMZ Group/VPN 4 WLAN Group/VPN		ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE) ESP 3DES HMAC SHA1 (IKE)		886 886 886

The 'VPN Policy' window will then appear. On the 'General' tab page, 'Security Policy' section, select "IKE using Preshared Secret" from the 'IPSec Keying Mode:' dropdown box.

VPN Policy - Microsoft Internet Explo	er					
General Network P	roposals	Advanced				
Security Policy						
IPSec Keying Mode:		IKE using Pres	shared Secret			
Name:		to_Checkpoint		_		
IPSec Primary Gateway Name or Ad	idress:	67.115.118.94				
IPSec Secondary Gateway Name or	Address:	0.0.0.0				
Shared Secret		HaRdI_to_Gue	65_805			
Local IKE ID (optional):	SonicWA	LL Identifier 💌	HUB-TEST	_		
Peer IKE ID (optional):	IP Addres	s 💌	192.168.170.1			
Ready						
			OK	Cancel	н	ыþ

Name: "to_checkpoint" IPSec Primary Gateway Name or Address: 67.115.118.94 Shared Secret: HaRd!_to_Gue55_B0b Local IKE ID: SNWL Identifier HUB-TEST (the SonicWALL Identifier needs to be identical as the VPN SA name on the CheckPoint NG) Peer IKE ID: IP Address 192.168.170.1



Next select the 'Network' tab.

đ١	VPN Policy - Microsoft Internet Explorer	_ 🗆 🗙
	General Network Proposals Advanced	
	Local Networks	
	Choose local network from list LAN Primary Subnet	
	O Local network obtains IP addresses using DHCP through this VPN Tunnel	
	C Any address	
	Destination Networks	
	C Use this VPN Tunnel as default route for all Internet traffic	
	Destination network obtains IP addresses using DHCP through this VPN Tunnel	
	Choose destination network from list checkpoint_group	
	Ready	
	OK Cancel Hel	
	OK Canter He	

In the 'Local Networks' section, select the radio button next to 'Choose local network from list' and select "LAN Primary Subnet" from the dropdown box.

In the 'Destination Networks' section, select the radio button next to 'Choose destination network from list' and select "checkpoint_group" from the dropdown box.

Next select the 'Proposals' tab. The default values should be correct, except the 'Life Time'; normally "28800" should be lowered to "3600" in both Phase 1 and 2 proposals. Verify that all values are correct.

٩Ì	VPN Policy - Microsoft Internet Explore	r			
	General Network Pro	posals Advance	d		
	IKE (Phase 1) Proposal				
	Exchange:	Aggressive Mode			
	DH Group:	Group 5	•		
	Encryption:	3DES	•		
	Authentication:	SHA1	×		
	Life Time (seconds):	3600			
	Ipsec (Phase 2) Proposal				
	Protocol:	ESP	•		
	Encryption:	3DES	۲		
	Authentication:	SHA1			
	Enable Perfect Forward Secrecy				
	DH Group:	Group 2	V		
	Life Time (seconds):	3600			
	Ready				
			OK	Cancel	Help

IKE (Phase 1) Proposal Exchange: Aggressive Mode

DH Group: Group 5 Encryption: 3DES Authentication: SHA1 Life Time (seconds): 3600



Ipsec (Phase 2) Proposal Protocol: ESP Encryption: 3DES Authentication: SHA1 DH Group Group 2 Life Time (seconds): 3600 Do not enable Perfect Forward Security.

Next select the 'Advanced' tab.

Advanced Settings	
Enable Keep Alive	
Require authentication of VPN c	lients by XAUTH
User group for XAUTH users:	Select a user group
Enable Windows Networking (N	letBIOS) Broadcast
Enable Multicast	
Apply NAT Policies	
Translated Local Network	Select Translated Local Network
Translated Remote Network	Select Translated Remote Network
Management via this SA:	Г НТТР Г НТТРЗ
User login via this SA:	F HTTP F HTTPS
Default LAN Gateway (optional):	0000
VPN Policy bound to:	Zone WAN

Make sure that the option Enable Keep Alive has been checked. All other options can be left as they are. Click the OK button.

This completes the settings on the SonicWALL TZ170 installed on Side Bob.



Check Point FireWall-1NG Setup

Log into SmartDashboard.

	elcome to Check Point martDashboard
🔲 <u>D</u> emo Mode	Basic (Firewall)
● <u>U</u> ser Name	admin
C Certificate:	
Password:	*****
<u>S</u> martCenter Server:	192.168.170.1
Read O <u>n</u> ly	More Options >>
<u>0</u> K	Quit

Before the VPN can be setup it is necessary to create Network Objects for all devices and networks. To create the network objects, first click on 'Manage' on the top of the SmartDashboard. Then click on 'Network Objects...' from the drop down box.

Wanherten.com - Check Point S Elle Edit View Manage Rules P								1×				
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0				♥ 🕹 🖪 🖽								
## XX I = 🏫 🔲 8= 1												
º+ << <> <> <> <> <> <> <> <> <> <> <> <>		14		fense 🔯 VPN Mana	ger 🔀 Desktop Securi	ky						
Network Objects Oneck Point	NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	-				
Nodes Interoperable Devices	Ī	∼ EncDomain HubG	~ EncDomain Spok	* Any Traffic	~ EncryptedService	Encrypt8Continue	- None					
Networks Groups	Ī	∼ MemberGWs Enc	∼ MemberGWs.Enc	* Any Traffic	∼ EncryptedService	Encrypt&Continue	- None					
Dynamic Objects	-	Accept VPN traffic	rule (configured fro	om the community)					Manage	Rules	Policy	Search
	•	* Any	🔆 Member Gatewar	🔆 HUB-TEST	~ Encrypted Servic	🔂 accept	🔳 Log		-	1.01.1		
	,	Hecc_P FamPeeters	💦 opmodule	* Any Traffic	TOP CPM TOP microsoft-ds	🔂 accept	🔳 Log		Netwo	rk Obje es	cts	2
	2	Cpmodule	* Any	* Any Traffic	* Any	💮 accept	E Log		Resou	rces		-
	з	* Any	TZ170	* Any Traffic	TOP https	🔂 accept	🔳 Log				ations	
	4	* Any	UanHertenServe	* Any Traffic	TOP Rtp TOP http	😨 accept	Log		Server	•••	300115	
	5	* Any		* Any Traffic	VEO_OBSERVER		🔲 Log				ninistrat	ors
	6	+ CP_LAN	blocked_P	* Any Traffic	* Any	🖲 drop	Log					0.0111
	7	+ CP_LAN	* Any	* Any Traffic	* Any	accept	Log		Permis	sions Pr	ofiles	
	0	* Any	* Any	* Any Traffic	* Any	i drop	Log	_	Time			
							2		VPN C	ommuni	ies	
or Help, press F1				va	nherten.com Rei	ad/Write NUM		10				

The 'Network Objects' window will then appear. The first object to create is for the LAN subnet of the Checkpoint FW, it's likely that these object already exist as they are used as the base for most rules. To create the LAN object, click the 'New' button at the bottom of the 'Network Objects' window, then select 'Network' from the dropdown box.

Network Objects			x
Network objects Show: All	:	▼ More >>	
AuxiliaryNet blocked_P CP_LAN comodule DMZNet dsl	I	•	
<u>N</u> ew	<u>R</u> emove	<u>E</u> dit	
<u>C</u> lose	Actions	<u>H</u> elp	

New F	Remove
Check Point	+
Node	•
Interoperable De	эчісе
Network	N
Domain	ĸ
OSE Device	
Group	
Logical Server	
Address Range.	
Dynamic Object.	
VoIP Domains	•



The 'Network Properties' window will then appear.

Network Properties -	CP_LAN		×
General NAT			,
<u>N</u> ame:	CP_LAN		
Network Address:	192.168.170.0		
Net <u>M</u> ask:	255.255.255.0		
<u>C</u> omment:			
Color:	-		
Broadcast addre	ss: C N <u>o</u> t included		
	OK Cance	l Help	ı

In this window, enter the object:

Name: CP_LAN Network Address: 192.168.170.0 Net Mask: 255.255.255.0

The next network objects to create are for the LAN of the SonicWALL appliance at Side Alice and for the LAN of the SonicWALL appliance at Side Bob.

From the 'Network Objects' window, click the 'New' button at the bottom of the 'Network Objects' window, then select 'Network...' from the dropdown box.

Here we create the Network Object for the LAN of Side Alice. Make sure that the Object contains the correct LAN Network Address and Net Mask. Within our example we used:

Name: Network_Alice Network Address: 180.10.10.0 Net Mask: 255.255.255.0

Network Properties	- Network_Alice	×
General NAT		
<u>N</u> ame:	Network_Alice	
Network Address	ε 180.10.10.0	
Net <u>M</u> ask:	255.255.255.0	
<u>C</u> omment:		
Cojor:		
Broadcast addr	C Ngt included	
	OK Cancel Help	



Here we create the Network Object for the LAN of Side Bob. Make sure that the Object contains the correct LAN Network Address and Net Mask. Within our example we used:

Name: Network_Bob Network Address: 10.234.234.0 Net Mask: 255.255.255

Network Properties	Network_Bob	×
General NAT		
<u>N</u> ame:	Network_Bob	
Network Address:	10.234.234.0	
Net <u>M</u> ask:	255.255.255.0	
Comment:		
Color:	-	
Broadcast addre	C Not included	
	OK Cancel	Help

Next, edit the 'Check Points' network object. It should be named the same as the machine name then press the edit button. If it does not exist, create it under 'New' > 'Check Point' > 'Gateway...' and proceed to the next step.

etwork Objects 🛛 🗙	I											
Network objects:	New	Remove		E dit	E dit	E dit	E dit	E dit	E dit	E dit	E dit	E dit
Show: Check Points More >>	Check Po	int 🔎	•	Gateway	Gateway	Gateway	Gateway	Gateway	Gateway	Gateway	Gateway	Gateway
	Node	1	·	Hast	Hast	Host	Host ¹ /S	Host 45	Hast 45	Hast 45	Hast 45	Hast 45
	Interope	rable Device		Gateway Clus	Gateway Cluster	Gateway Cluster	Gateway Cluster	Gateway Cluster	Gateway Cluster	Gateway Cluster	Gateway Cluster	Gateway Cluster
	Network			Embedded Da	Embedded Device	Embedded Device	Embedded Device	Embedded Device	Embedded Device	Embedded Device	Embedded Device	Embedded Device
	Domain			Externally Ma	Externally Managed	Externally Managed Gat	Externally Managed Gatew	Externally Managed Gateway				
	OSE Dev	ice		Externally Ma	Externally Managed	Externally Managed Ho:	Externally Managed Host	Externally Managed Host	Externally Managed Hast	Externally Managed Host	Externally Managed Host	Externally Managed Host
	Group	,										
	Logical 5	erver										
<u>New</u> <u>R</u> emove <u>E</u> dit	Address	Range										
Close Actions <u>H</u> elp	Dynamic	Object										
	VoIP Don	nains I	•									



The 'Check Point Gateway' page will appear. On 'General Properties', verify the 'IP Address' and that both 'FireWall-1' and 'VPN-1 Pro' are selected. In this example, the 'IP Address' is "192.168.170.1". When finished, click 'Topology' on the left hand side.

	Check Point Gateway - General Properties	
⊡ ··· Topology ···· NAT ⊡ ·· VPN	Name: cpmodule	
Remote Access	IP Address: 192.168.170.1 Get address Dynamic Address	
Authentication Logs and Masters Capacity Optimization Advanced	Comment:	
	Cojor:	
	Check Point Products	
	Version: NG with Application Intelligence Get Version	
	Type: Check Point Enterprise/Pro	
	Firewall VPN Oos SecureClient Policy Server SecureClient Station Veh Management Station Additional Products: Web Server Secure Internal Communication Communication DN: cn=cp_mgmt.o=cpmodule.5z8yy6	

On 'Topology', verify the network addresses of the 'internal' and 'external' networks listed under the 'Topology' section. If nothing is populated in the topology fields, click 'Get Topology...'

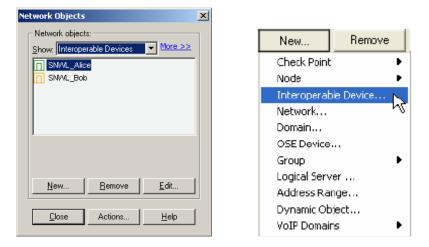
Check Point Gateway - cp	module
Check Point Galaxies of Control Contro	Name P Address Det P Address Name P Address eh1 6/11511834 255252525 External eh1 6/11511834 Edt Bemove
	OK Cancel Hab

In this example: External network: "67.115.118.94" Net mask : "255.255.255.255" Internal network: "192.168.170.1" Net mask: "255.255.255.0" (internal is also referred to as 'This Network').

In the 'VPN Domain' section select 'Manually defined' and select the previously created "CP_LAN" Network Object with the dropdown menu. When this is done you can close this page by pressing the OK button.



It is needed to create also Interoperable Network objects for the both SonicWALL appliances. Go to 'Manage' > 'Network Objects' now the Network Objects window will then appear. To create the 'Interoperable Device' object, click the 'New' button at the bottom of the 'Network Objects' window, then select 'Interoperable Device' ...' from the dropdown box. The 'Interoperable Device' window will then appear.



In this window, under 'General Properties' enter Name: SNWL_Alice IP Address: 207.88.91.77 Next click 'Topology' on the left hand side.

Interoperable Device - SN	WL_Alice	×
General Properties Topology		
	Name: SNWL_Alice	
	IP Address: 207.88.91.77 Get address	
	Comment:	1
	Cojor:	
	· ,	
1		
	OK Cancel Help	



On the 'Topology' page, under the 'VPN Domain' section, select 'Manually defined' and select the previously created "Network_Alice" Network Object with the dropdown menu. Click on 'OK' to finish.

An Interoperable Device Object needs also to be created for Side Bob. Go to 'Manage' > 'Network Objects' now the Network Objects window will then appear. To create the 'Interoperable Device' object, click the 'New' button at the bottom of the 'Network Objects' window, then select 'Interoperable Device' ...' from the dropdown menu.

VPN	<u><u>G</u>et</u>			
	Name I	P Address	Network Mask	IP Addresses behind interface
	<u>, - , </u>			
	<u>A</u> dd	<u>E</u> dit.	<u>R</u> emove	
	VPN Doma	in ———		
			Gateway based on T	opology information.
		ddresses <u>b</u> ehind		
		ddresses <u>b</u> ehind	Gateway based on T 나나 Network_Alic	
		ddresses <u>b</u> ehind		
		ddresses <u>b</u> ehind		
		ddresses <u>b</u> ehind		

The 'Interoperable Device' window will then appear.

Interoperable Device - SN	WL_Bob	×
General Properties		
Topology		
⊡ · VPN	Name: SNWL_Bob	
	IP Address: 80.62.91.20	
	Comment:	1
	Cojor:	
	OK Cancel Help	



In this window, under 'General Properties' enter: Name: SNWL_Bob IP Address: 80.62.91.20 Next click 'Topology' on the left hand side.

On the 'Topology' page, under the 'VPN Domain' section select 'Manually defined' and select the previously created "Network_Bob" Network Object with the dropdown menu. Click on 'OK' to finish.

Interoperable Device - SNW	L_Bob	×
General Properties	Тороlоду	
Topology Topology Topology	<u>G</u> et	
	Name IP Address Network Mask IP Addresses behind interface	
	Add	
	VPN Domain O All IP Addresses behind Gateway based on Topology information.	
	Adul P Addresses penind Gareway based on Topology information. Manually defined	
	OK Cancel Help	

Now all the Network Addresses are created which will be needed to setup the VPN SA on the Checkpoint NGAI unit. Next, define the VPN. From the top menu, select 'Manage' and then 'VPN Communities...'; the 'VPN Communities' window will appear.

🖀 vanherten.com - Check Point SmartDashboard - VPN Manager	_ 8 ×
Elle Edit Yew Manage Rules Policy Search Window Help	
🗣 🔍 🕼 💫 🙃 🧱 Security 🖽 Address Translation 🚇 SmartDefense 🔞 VPN Manager 🛗 Desktop Security	
E Q. Network Objects	
Hub-TEST MyIntranet RemoteAccess	
Retworks	
Terring Groups Terring Groups Terring Groups Terring Groups Terring Groups	
B to the Dynamic Ubjects	
	₹) ≜
SNWL_Bob cpmodule SNWL_Alia	ce
	*
For Help, press F1 vanherten.com Read/Write NUM	



From the 'VPN Communities' window, select the 'New' button on the bottom. Then select 'Site To Site' and 'Star...' The 'Star Community Properties' page will appear.



On the 'Star Community Properties' page, enter the VPN name in the 'Name:' field. In this example, the 'Name:' is "HUB-TEST" which needs to be the same as the SNWL Identifier setup in the VPN SA on the Spokes.

Star Community Propertie	es - HUB-TEST	×
Star Community Propertia General - Central Gateways - Satelite Gateways - Excluded Services - VPN Properties - Advanced Properties - Shared Secret	ss - HUB-TEST General Name: HUB-TEST Color: Color: Enable VPN routing for satelites: To center only Context and to other satelites through center To center only Context and to other satelites through center Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and other Context and the center to other satelites, to internet and t	X
	Community Traffic Security Policy Accept all encrypted traffic. Note: The rule applies for all Internally Managed community members.	-
	Note: The fulle applies for all internally managed community memoers.	1
,	OK Cancel Help	

For the 'Enable VPN routing for satellites' you need to select the option 'To center, or through the center to other satellites, to internet and other VPN targets.'

At the Community Traffic Security Policy it is necessary to have the checkbox 'Accept all encrypted traffic' ticked. Next, click on 'Central Gateways'.

On the Central Gateways, click on the 'Add...' button under the 'Central Gateways:' section. This will bring up the 'Central Gateways' window. Select here the address object 'cpmodule' and press OK.



Star Community Propertie	25 - HUB-TEST	×	
General Central Galeways Satellic Galeways Excluded Services Advanced Properties Shared Secret	Central Gateways Add		Add Central Gateways Add Central Gateways For comodule The candidates must be defined as: VPN-1 installed. Version NG FP1 and above (Only for Internally managed). Host, Gateway, Gateway Cluster or Interoperable Device
	OK Cancel Help		OK Cancel Help

Next, click on 'Satellite Gateways'. On the Satellite Gateways, click on the 'Add...' button under the 'Satellite Gateways' section. This will bring up the 'Satellite Gateways' window.

	Star Community Properties - HUB-TEST
Add Satellite Gateways SNML_Alice SNML_Bob The candidates must be defined as: 1. VPN-1 installed. 2. Version NG FP1 and above (Only for Internally managed). 3. Host, Gateway, Gateway Cluster or Interoperable Device	Start Community Properties Statellite Gateways Seteral Gateways Statellite Gateways Schuded Services -PK Properties Shared Secret SMMAlice SMMBob New
OK Cancel Help	OK Cancel Help

Select here the address objects 'SNWL_Alice' and address object 'SNWL_Bob' after this is done press OK.



Click on 'VPN Properties'.

r Community Propertie	S - HOD-ILST			[
; General	VPN Properties			
- Central Gateways - Satellite Gateways	IKE (Phase 1) Properties			
Excluded Services	Derfore her enderner enemetien with	2050		
Advanced Properties	Perform key exchange encryption with:	3DES	<u> </u>	
Shared Secret	Perform gata integrity with:	SHA1	~	
	IPsec (Phase 2) Properties			
	Perform IPsec data encryption with:	3DES	<u>•</u>	
	Perform gata integrity with:	SHA1	•	
	OK	Cancel	Help	

Enter the 'IKE (Phase 1) Properties' and the 'IPsec (Phase 2) Properties'. In this example, the 'IKE (Phase 1)' section the settings are as follows:

IKE (Phase 1) Properties

Perform key exchange encryption with: 3DES Perform data integrity with: SHA1

Ipsec (Phase 2) Properties

Perform IPsec data encryption with: 3DES Perform data integrity with: SHA1

Next, click on 'Advanced Properties.'

Star Community Propertie	s - HUB-TEST	X
General Central Gateways	Advanced Properties	
 Central Gateways Satellice Gateways Excluded Services VPN Properties Advanced Properties Advanced Properties Shared Secret 	IKE (Phase 1) Use Diffie Hellman group: Group 5 (1536 bit) ▼ Benegotiate IKE security associations every 60 ➡ minutes ✓ Use aggressive mode IPsec (Phase 2) Uge Diffie Hellman group: Group 2 (1024 bit) ▼ Benegotiate IPsec security associations every 3600 ➡ seconds C Support Site to Site IP compression	
	NAT	



In the 'Advanced Properties' section, under IKE (Phase 1), modify the 'Renegotiate IKE security associations every' field to "60" minutes and the 'Use Diffie-Hellman group' should be "Group 5 (1536 bit). Tick the option 'Use aggressive mode' For the 'Ipsec (Phase 2) Proposal' section the settings are as follows: 'Life Time (seconds)' is "3600". Do not enable Perfect Forward Security. At the 'NAT' it is necessary to tick the option 'Disable NAT inside the VPN community'

Click 'Shared Secret'.

General	Shared Secret		
- Central Gateways - Satellite Gateways - Excluded Services - VPN Properties - Advanced Properties - Shared Secret	Each External memb	ecret for all External members er will have the following I members in this community.	
	Peer Name	Shared Secret	
	SNWL_Alice SNWL_Bob	800X	
	<u>E</u> dit	<u>R</u> emove	

On the 'Shared Secret' section, tick the option 'Use only Shared Secret for all External members'. Highlight "SNWL_Alice" in the 'Peer Name' table below. Click on the 'Edit..." button to enter the secret. In this example, the shared secret is "HaRd!_to_Gue55_Al1c3" press the OK button. After this Highlight "SNWL_Bob" in the 'Peer Name' table below. Click on the 'Edit..." button to enter the secret is "HaRd!_to_Gue55_B0b" and press the OK button.

Insert Secret		X
Enter secret:	HaRd!_to_Gu	
OK		Cancel

Click 'OK' to finish the VPN Interoperability Hub Spoke setup between the SonicOS 2.5 Enhanced and Checkpoint NG within the SmartDashboard. Make sure that the Policy has been installed onto the Checkpoint firewall to have it working.

Document Created: 11/16/2004 Last Updated: 06/19/2008 Version 1.1

